Contents

1 Introduction **6**

2 RSA and Lattices **13**
2.1 The RSA cryptosystem 13
2.2 Preliminaries on lattices 21

3 Coppersmith's method **24**
3.1 Introduction 24
3.2 The univariate case 27
3.3 Applications of Coppersmith's method in the univariate case 39
3.4 The multivariate case 44

4 Weak Keys in RSA **49**
4.1 Introduction 49
4.2 Wiener's attack 54
4.3 Generalizing Wiener's attack 59
4.4 An application – Cryptanalysis of the YKLM-scheme 66
4.5 There are $N^{\frac{3}{4}-\epsilon}$ weak keys 69

5 Unbalanced RSA with Small CRT-Exponent **77**
5.1 Introduction 77
5.2 An approach for $q < N^{\frac{1}{3}}$ 81
5.3 Improving the bound to $q < N^{0.382}$ 85
5.4 An approach that allows larger values of d_p 89
5.5 Comparison of the methods 93

6 Knowing A Fraction of the Secret Key Bits **95**
6.1 Introduction 95
6.2 MSBs known: A method for $e \in [N^{\frac{1}{2}}, N^{\frac{\sqrt{6}-1}{2}})$ 105
6.3 LSBs known: A provable method for $e < N^{\frac{1}{2}}$ 111
6.4 LSBs known: A method for all e with $e < N^{\frac{7}{8}}$ 115
6.5 Known MSBs/LSBs and Chinese Remaindering 119

6.6 Considering moduli of the form $N = p^r q$ 121
6.6.1 Partial key exposure attacks from new attacks for small d 122
6.6.2 Attacks for small d modulo $p - 1$ 129

7 Improved Lattice Bases **132**
7.1 Introduction 132
7.2 The Boneh-Durfee lattice 135
7.3 A new method for selecting basis vectors 137
7.4 Application of the method 146
7.5 A case where the resultant heuristic fails 151